

From:	Avinoam Brog <broga@mwi.co.il>
To:	ehbarak1@gmail.com
CC:	
Date:	Mon, 1/26/2015 2:23:16 PM
Subject:	FW: ICT Cyber-Terrorism Activities Report No. 10

Avinoam Brog
Chairman of the Board
Ipsos (Israel)



13 Tuval St., Ramat Gan, Israel

Tel: + 972 3 7533333 Direct: +972 3 7533330 Mobile: +972 +50 4404704

broga@mwj.co.il www.ipsos.com

The Home of Researchers



Please consider the environment before printing this e-mail. 

<http://www.youtube.com/watch?v=FM9kCfFrhRg>

From: ICT: International Institute for Counter-Terrorism [mailto:ict@idc.ac.il]

Sent: Sunday, January 25, 2015 2:30 PM

To: Avinoam Brog

Subject: ICT Cyber-Terrorism Activities Report No. 10

View this email [in your browser](#)



ICT Cyber-Desk

PERIODIC REVIEW

Cyber-Terrorism Activities Report No. 10

By ICT Cyber Desk Team

[Please click here to view the full ICT Cyber-Terrorism Activities Report](#)

This report covers the period of July - September 2014, and covers two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse) and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack).

The following are among the issues covered in this report:

- Documentation of training videos and written tutorials on the topics on cyber-security and protection. The discourse concerned intelligence efforts to identify cyber-criminals online and included explanations on how to surf the Web anonymously using various software programs and techniques.
- A group of hackers called the "Islamic State Electronic Battalions" claimed responsibility for the breach of Twitter accounts belonging to "White Shroud", an organization that operates against the Islamic State in Syria-Iraq.
- During Operation 'Protective Edge' there was an increase in attempted cyber-attacks against Israeli targets in the framework of the OpIsrael and OpSaveGaza operations, including a breach of the IDF spokesperson's Twitter account and a fictitious announcement regarding a feared nuclear leak in the Dimona area.
- There was an increase of cases in which the details of millions of credit cards used at retail chains throughout the United States were leaked, from the start of 2013 and throughout 2014, which caused lasting economic damage.
- There was an increase on the usage of darknet-based malware in an effort to increase the anonymity of the user in carrying out an attack. The malware, which uses TOR and I2P, encrypts data traffic between the attacked computer and the control and command server.

[Click here for the Cyber-Terrorism Activities Report No. 10](#)

The ICT Cyber Desk Review is a periodic report and analysis that addresses two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse); and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack). The Cyber Desk Review addresses the growing significance that cyberspace plays as a battlefield in current and future conflicts, as shown in the recent increase in cyber-attacks on political targets, crucial infrastructure, and the Web sites of commercial corporations.

For a list of the ICT Cyber Desk Team reviews available to the public, [click here](#)
For tailored research please contact us, at [cyber](#)



To be removed from our mailing list go [here](#)
International Institute for Counter-Terrorism, POB: 167, Herzeliya,
46150, Israel
Copyrights © all rights reserved

ICT -International Institute for Counter-Terrorism

[אקטיב-טרייל](#) נשלח באמצעות תוכנת